

SUMMONS ISSUED

Bernard Daskal  
LYNCH DASKAL EMERY LLP  
264 West 40th Street  
New York, New York 10018  
(212) 302-2400

**FILED**  
IN CLERK'S OFFICE  
U.S. DISTRICT COURT E.D.N.Y.

★ DEC 13 2011 ★

BROOKLYN OFFICE

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

-----X  
DAVID YASTRAB, Individually and on Behalf : Civil Action No.:  
of All Others Similarly Situated, :

Plaintiff, :

CLASS ACTION COMPLAINT

-against- :

CARRIER IQ, INC. and HTC AMERICA, INC., :

Defendants. :

11-6069

FEUERSTEIN, J.

WALL, W.

Plaintiff David Yastrab (“Yastrab” or “Plaintiff”), by his undersigned attorneys, Lynch Daskal Emery LLP, on behalf of himself and all similarly situated persons (the “Class,” as defined below, ¶44), brings this action against defendants Carrier IQ, Inc. (“Carrier”) and HTC America, Inc., (“HTC”) (collectively, “Defendants”) and alleges:

### **NATURE OF THE ACTION**

1. This class action complaint seeks relief available to Plaintiff and the putative class he seeks to represent pursuant to the Omnibus Crime Control and Safe Streets Act of 1968, also known as the Federal Wiretap Act, 18 U.S.C. §2510 et seq. (the “Federal Wiretap Act”).

2. Upon information and belief, Carrier’s software is installed on more than 141 million mobile devices. The Carrier software, as alleged below, allows Defendants to improperly and/or unlawfully access, intercept or collect consumers’ personal electronic communications and information, including, for example, customer location, internet web searches, text messages, etc. from private mobile phones or devices (“Mobile Phones”) belonging to Plaintiff and members of the Class.

3. As a result, Defendants violated (and are in violation of) the Federal Wiretap Act by accessing, intercepting, and/or collecting personal electronic communications and information, belonging to customers, from consumers’ Mobile Phones.

4. An online distribution of a study by a Connecticut-based technology officer revealed that the Carrier IQ software is recording private and sensitive information, without the knowledge or consent of the mobile device users, from consumers’ Mobile Phones.

5. Moreover, on November 30, 2011 the United States Committee on the Judiciary wrote to Carrier IQ demanding material, data or information relating to the software’s tracking capabilities. The letter states that Carrier’s actions “may violate federal privacy laws, including the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act.”

6. HTC was and continues to be prohibited from wrongfully accessing, intercepting, and/or collecting any personal electronic communications and information from Plaintiff and members of the Class.

7. Notwithstanding, Defendants accessed, intercepted, and/or collected personal electronic communications and information belonging to Plaintiff and members of the Class. HTC deployed Carrier IQ software as a pre-installation on its mobile devices and allowed it to be used to access, intercept or collect personal electronic communications and information belonging to Plaintiff and the Class.

8. This suit seeks equitable relief and damages on behalf of Plaintiff and the Class.

#### **PARTIES**

9. Plaintiff David Yastrab resides at 244 Steven Place in Woodmere, New York (Nassau County). Defendants had access to Plaintiff's personal electronic communications and information through his ownership of a HTC mobile device. Plaintiff purchased his Mobile Device, a HTC Incredible, in or about July 2011. Plaintiff has not consented to the use of his private/sensitive information, as alleged herein, by Defendants.

10. Carrier, a provider of mobile services intelligence solutions, is a privately-owned company headquartered at 1200 Villa Street, Suite 200 in Mountain View, California.

11. Defendant HTC America, Inc. is incorporated in the State of Washington and headquartered at 13920 SE Eastgate Way, Suite 400 in Bellevue, Washington.

#### **JURISDICTION AND VENUE**

12. This Court has original jurisdiction over this matter pursuant to 28 U.S.C. §1331.

13. Venue properly lies in this District pursuant to 28 U.S.C. §1391(a). Plaintiff and Defendants reside, are found, have an agent, or have transacted substantial business within the

Eastern District of New York and a substantial part of the events giving rise to the claims alleged herein occurred in the District.

14. This Court also has original jurisdiction over this matter, pursuant to 28 U.S.C. §1332(d), in that the matter in controversy exceeds \$5 million, exclusive of interest and costs, and is a class action of more than 100 potential Class members in which the citizenship of at least one proposed Class member is different from that of at least one defendant.

### **SUBSTANTIVE ALLEGATIONS**

15. Plaintiff owns a Mobile Device manufactured by HTC.

16. In connection with the manufacture and sale of its Mobile Phones, Defendants had access to personal electronic communications and information belonging to Plaintiff and Class members.

17. Defendants unlawfully accessed, intercepted, and/or collected the personal electronic communications and information belonging to Plaintiff and members of the Class in violation of those laws designed specifically to protect consumers and the general public.

18. Carrier IQ's software, which is embedded in tens of million Mobile Phones, was and is logging information such as location and key strokes – without notifying users.

19. Carrier self-describes its software “[a]s the only embedded analytics company to support millions of devices simultaneously” and that, through this capability, it gives wireless carriers and handset manufacturers “unprecedented insight into their customers’ mobile experience.” In fact, Carrier’s software is generally classified as “rootkit” software – rootkit software is an industry term used to describe software that enables continuous access to a computer’s privileged information while hiding the software’s presence.

20. Carrier IQ, upon information and belief, is capable of monitoring key pressed or hardware keys, app opened, sms received, screen off or on, call received, media statistics and

location statistics. Once the information is obtained from the phone, it is electronically sent to and maintained by Carrier and/or its customers.

21. HTC develops and markets a variety of mobile wireless devices and has sold tens of millions mobile phones and devices worldwide. HTC's wireless phone business includes the manufacture and sale of Android smartphones.

22. HTC's Android smartphone devices are embedded with Carrier IQ software. Specifically, HTC Android smartphone users have the Carrier IQ software embedded in their mobile devices and Defendants have access to their personal electronic communications, information, and other usage data.

23. Defendants used the Carrier IQ rootkit software, upon information and belief, to improperly access, intercept, and/or collect the data containing personal electronic communications and information without the mobile user's knowledge or consent. In turn, the interception of personal electronic communications and information by the Carrier IQ rootkit created the opportunity for the permanent recordation of the data.

24. Accordingly, Carrier IQ clients, including HTC, its manufacturer competitors and wireless carriers, have (and/or could have) direct access to the personal electronic communications and information of its mobile device users. And, as a result, mobile device users' intrinsic and legal right to the protection and privacy of their personal electronic communications and information was removed through the access, interception and/or collection by third parties.

25. Senator Al Franken, Chairman of the Subcommittee on Privacy Technology and the Law, stated his concern about the Carrier rootkit functionality in a letter to Carrier IQ. He said that "it appears that Carrier IQ's software captures a broad swath of extremely sensitive information from users that would appear to have nothing to do with diagnostics—including who they are calling, the

contents of the texts they are receiving, the contents of their searches, and the websites they visit. Senator Franken went so far as to state that “[t]hese actions may violate federal privacy laws, including the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act.”

**Applicable Law**

26. The Federal Wiretap Act, 18 U.S.C. §2511, provides that “any person who—(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . shall be punished . . . or subject to suit.”

27. Here, Defendants have access to personal electronic communications and other information belonging to mobile device users and, in effect, are subject to the Federal Wiretap Act. Based on the allegations above, Defendants violated the Federal Wiretap Act through their interception of the personal electronic communications (and other information) belonging to Plaintiff and the members of the putative Class he seeks to represent.

28. The Federal Wiretap Act, 18 U.S.C. §2520, specifically provides:

any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter . . . may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

In an action under this section, appropriate relief includes—(1) such preliminary and other equitable or declaratory relief as may be appropriate; (2) damages under subsection (c) and punitive damages in appropriate cases; and (3) a reasonable attorney’s fee and other litigation costs reasonably incurred.

[T]he court may assess as damages whichever is the greater of—(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or (B) statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000.

29. The Carrier IQ rootkit software is not in compliance with this federal law.

### CLASS ACTION ALLEGATIONS

30. This action is brought as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

31. Plaintiff, both in his individual capacity, and in his representative capacity as a member of the Class, brings this action against Defendants, on behalf of all persons in the United States whose personal electronic communications and information are or were unlawfully intercepted or collected by HTC through the use of Carrier IQ software preinstalled on its Android smartphone devices.

32. The Class consists of those persons who were or are owners of HTC Android smartphone devices.

33. The members of the Class are so numerous that joinder of all members is impracticable.

(a) The exact number of Class members is unknown to Plaintiff at this time and can only be ascertained through appropriate discovery. Plaintiff believes, however, that there are more than tens of millions of members of the proposed Class.

34. Common questions of law and fact exist as to all Class members and predominate over any questions which affect only individual Class members. These common questions of law and fact include:

(a) Whether Defendants use the personal electronic communications or information in violation of the Federal Wiretap Act;

(b) Whether Defendants access, intercept, and/or collect the personal electronic communications or information in violation of the Federal Wiretap Act;

(c) Whether Defendants transmit the personal electronic communications and information from mobile users phones to Carrier IQ, HTC, wireless carriers, or other third parties; and

(d) Whether Plaintiff and the Class have sustained damages, and, if so, what is the proper measure of damages.

35. Plaintiff's claims are typical of the claims of the Class he seeks to represent in that Plaintiff and each Class member sustained, and continue to sustain, damages arising from Defendants' wrongdoing.

36. Plaintiff will fairly and adequately protect the interests of those Class members he seeks to represent and has no interests that are antagonistic to the interests of any other Class member.

37. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, since joinder of all the individual Class members is impracticable. Furthermore, because the damages suffered, and continued to be suffered, by each individual Class member may be relatively small, the expense and burden of individual litigation would make it very difficult or impossible for individual Class members to redress the wrongs done to each of them individually and the burden imposed on the judicial system would be enormous.

38. In addition, the prosecution of separate actions by the individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

39. Excluded from the Class are Defendants, including any entity in which Defendants have a controlling interest, or which is a parent or subsidiary of, or which is controlled by, any Defendant, and the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, or assigns of any Defendant.

## **COUNT I**

### **Violation of the Federal Wiretap Act, 18 U.S.C. §2510 et seq.**

40. Plaintiff hereby incorporates by reference the allegations contained in paragraphs 15 through 39 of this complaint.

41. Defendants were and are communication common carriers as defined, described or termed in the Federal Wiretap Act. *See* 18 U.S.C. §2510; 47 U.S.C. §151.

42. Plaintiffs and the members of the Class were and are, as mobile device users and parties to electronic communications, entitled to the protection of the Federal Wiretap Act

43. Upon information and belief, Defendants have (and continue to) intentionally intercept the personal electronic communications of Plaintiff and members of the Class.

44. As a proximate result of Defendants' improper interception and/or collection of the personal electronic communications and information, the Class has suffered a legally cognizable loss or injury.

45. The losses sustained by the Class are directly attributable to Defendants' wrongful conduct and were entirely foreseeable.

## **PRAYER FOR RELIEF**

Wherefore, Plaintiff requests the following relief, on behalf of himself and the Class:

A. An order declaring the actions complained of herein to be in violation of the statutory law set forth above, including a preliminary injunction enjoining Defendants from further acts in violation of the Federal Wiretap Act, pending the outcome of this action;

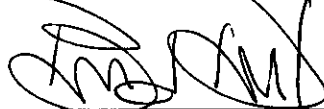
- B. An order enjoining and restraining Defendants from any further acts in violation of the Federal Wiretap Act set forth above;
- C. An award of compensatory damages in an amount deemed appropriate by the trier of fact against Defendants;
- D. An award of prejudgment and post-judgment interest;
- E. An award of costs, including, but not limited to, discretionary costs, attorneys' fees and expenses incurred in prosecuting this case; and
- F. Certification of this action as a class action, appointment of Plaintiff as a Class representative and the undersigned counsel as Class counsel;
- G. Any other and further relief to which Plaintiff and the Class may be entitled at law or in equity that this Court deems just and proper.

**JURY DEMAND**

Plaintiff and the Class demand a trial by jury on all issues so triable.

Dated: New York, New York  
December 13, 2011

LYNCH DASKAL EMERY LLP



By: Bernard Daskal (BD-9263)

264 West 40<sup>th</sup> Street  
New York, NY 10018  
Phone: (212) 302-2400  
Fax: (212) 302-2100  
Email: Daskal@lawlynch.com

*Attorneys for Plaintiff*